ARTICLE APPEARED
ON PAGE A26

THE NEW YORK TIMES
19 April 1978

Media
SSCI

Senate Panel Asks Role for Security Agency in Cryptography Grants

By MALCOLM W. BROWNE

The Senate Select Committee on Intelligence recommended yesterday that the National Security Agency, one of the main Government intelligence organizations, be given a formal role in the selection of private institutions and scientists for Federal research grants in cryptography and cryptanalysis.

The committee also exonerated the agency of allegations made by various computer scientists last year that private reseachers had been harassed and threatened by the agency. The N.S.A. is the nation's highest authority on secret codes.

Scientists expressed concern over the Senate report, asserting that the proposal to include intelligence officials in groups responsible for awarding research grants could result in a "dangerous" conflict of interest.

The controversy began when the National Bureau of Standards moved to insure the privacy of information stored in computers by developing a Federal standard.

What Standard Provides

The standard, which was promulgated at the beginning of this year, stipulates that computers containing private information must be "locked" by having the information stored in the form of a mathematical code.

The "key" to unlock the information is defined as a computer number (consisting only of zeros and ones) 56 units long, known only to authorized users of the information.

This coding system was proposed by the International Business Machines Corporation in consultation with the National Security Agency.

Among the most prominent critics of the new privacy standard was Dr. Martin E. Hellman, a computer scientist at Stnford Univesity. He charged that the 56-bit "key" was not long enough to provide real security, and that powerfu computers that could break the code could be built soon.

Another Code Developed

He and some of his colleagues further charged that the N.S.A. had brought pressure on the International Business Machines Corporation and the National Bureau of Standards to adopt the 56-bit system, which would not be too difficult for the intelligence agency to crack if security interests required it.

Dr. Hellman and his associates have developed another type of code that they regard as essentially undecipherable. It has been developed further by Dr. Ronald L. Rivest and his team at Massachusetts Institute of Technology and has been issued a patent.

Computer scientists engaged in code research were alarmed last fall by a letter sent by Joseph A. Meyer, an employee of the National Security Agency, to a professional journal. The published letter warned that computer scientists working outside the Government who published articles about their code research might be violating the Munitions Control Act.

Scientists said at the time that Mrl Meyer's letter implied a threat and a constraint on free research.

The published concern of various scientists and the replies from Government officials created a heated dispute in the pages of a number of scientific journals, notably Science.

Soon after the charges were made public, the Senate committee, headed by Senator Birch Bayh of Indiana, began hearings on the subject.

Summary Is Released

The committee's report is classified as secret, but a nine-page unclassified summary was released yesterday.

The report found no wrongdoing in the fact that the N.S.A had been called in for advice in framing the new computer privacy measure, called (Data Encryption Standard) in view of the agency's expertise in codes.

It concluded that Mr. Meyer had written his letter on his own and not under instructions from his agency. Furthermore, it concluded that the agency was not guilty of harassing scientists or bringing pressure on the National Science Foundation to withhold funds from scientists involved in code research.

The agency had expressed "concerned to N.S.R. about certain grants with cryptological ramifications," the report acknowledged, but the committee saw nothing improper in this.

The report criticized the "vagueness and ambiguity" of Federal regulations relating to cryptology and recommnded that Congress clarify them by law.

Key Reduced in Size

The new Nederal standard on data encryption was developed by I.B.M. after the National Security Agency "convinced I.B.M. that a reduced key size was sufficient," the report said. Originally, the corporation had proposed that the key required to unlock computerized information be a number 128 bits long, instead of the 56-bit number finally adopted.

In conclusion, the report said that "N.S.A. and N.S.F. should discuss the need for N.S.A. to become part of N.S.F.'s peer-review process of the review of grant proposals for research in cryptography or cryptanalysis."

Dr. Hellman, reached by telephone, said when first learning of the report that the last recommendation could result in a conflict between the interests of scientific research and Federal intelligence. But later in talking with officials of the National Science Foundation, he said, he was reassured by them that the arrangement would not stand in the way of research.

He and Dr. Rivest at M.I.T. also reiterated their belief that the new Federal computer code standard was too weak.

"The length of the key could easily have been doubled at no extra cost, as I.B.M. originally proposed," Dr. Rivest said. "If that had been done, no one now would be questioning the security of the key against attack by some big new computer of the future."

He said that he concurred with a number of other parts of the report, however, notably the need for formal clarification of Federal regulations on cryptography and code research.